CLAIMS

1. A method for protecting the contents of an electronic document, comprising:

confusing characters belonging to an electronic input document through an invertible scrambler to obtain a confused document; and

diffusing said confused document by mixing it with chaotic characters to obtain an encrypted document.

2. The method according to claim 1, characterized in that said confusing step comprises carrying out operations defined within a Galois field.

3. The method of claim 1 wherein said electronic input document comprises a plurality of strings of characters to be encrypted, and said confused document comprises a plurality of confused characters, and said confusing step comprises adding each string of characters to be encrypted to strings of confusing characters obtained by multiplying said strings of confused characters by respective multiplication constants.

4. The method of claim 3 wherein, before being multiplied by said multiplication constants, said strings of confused characters are delayed.

5. The method of claim 1, in which said confused document comprises a plurality of strings of confused characters, and said diffusing step comprises generating chaotic characters through a chaos generator and mixing said strings of confused characters with said chaotic characters.

6. The method of claim 5 wherein said mixing step comprises performing an exclusive OR operation.

7. The method of claim 5 wherein said chaos generator implements the function:

$$f_k(x)=Kx(1-x).$$

8. The method of claim 1, further comprising:

a) loading encryption keys into shift registers of said invertible scrambler and an initial chaotic value into a chaotic-value register;

b) acquiring an input character string;

c) calculating a diffused character string using said input character string, said encryption keys, and the contents of said shift registers;

d) feeding said diffused character string to said shift registers, and issuing a command for a shift operation for said shift registers;

e) repeating b), c) and d) a preset number of times to obtain a plurality of said confused character strings;

f) calculating a subsequent chaotic value, using the contents of said chaotic value register;

g) adding said plurality of confused character strings to said subsequent chaotic value to obtain an encrypted word;

h) storing said subsequent chaotic value in said chaotic value register; and

i) repeating b)-h).

9. The method of claim 8 wherein c) uses the following relation:

$$s(t) = IN(t) \oplus \sum_{j=0}^{3} c_j \oplus s(t-j)$$

in which *IN(t)* is said input character string, c_j are said encryption keys, $s(t-j)$ are the contents of said shift registers, and *s(t)* is said diffused character string.

10. The method of claim 8 wherein f) uses the following relation:

$$f_k(x)=Kx(1-x);$$

where K is a bifurcation parameter of a chaotic system.

11. The method of claim 1, comprising decrypting an encrypted document by mixing it with said chaotic characters and unscrambling through an unscrambler opposite to said scrambler.

12. to the method of claim 3, in which an encrypted document comprises a plurality of encrypted character strings, the method comprising decrypting said encrypted document through a first and a second decryption operation, in cascade, said second decryption operation supplying a plurality of decrypted character strings, said first decryption operation comprising a mixing step wherein said encrypted character strings are mixed with said chaotic characters to obtain a plurality of predecrypted character strings, and said second decryption operation comprising an unscrambling step by subtracting each predecrypted character string from feedback character strings obtained by multiplying said decrypted character strings by said multiplication constants.

13. A device for protecting the contents of an electronic document, comprising:

a confusion block for confusing an electronic input document, said confusion block comprising an invertible scrambler that supplies a confused document; and

a diffusion block cascade-connected to said confusion block, said diffusion block comprising mixing means for mixing said confused document with chaotic characters, which supply an encrypted document.

14. The device of claim 13 wherein said scrambler comprises operators acting within a Galois field.

15. The device of claim 13 wherein said scrambler comprises an adding element having a first and a second input, said first input receiving a string of characters to be encrypted that belong to said electronic input document; a plurality of shift registers cascade-connected to one another and to said adding element; a plurality of multiplier elements, each having an input connected to an output of a respective shift register and to an own output; a plurality of adding nodes cascade-connected, each adding node having an input connected to said output of a respective multiplier element, an adding node arranged upstream and having a second input connected to a last multiplier element of said multiplier elements, and an adding node arranged downstream and having an output connected to said second input of said adding element.

16. The device of claim 13 wherein said mixing means comprise an EXOR logic circuit, and said diffusion block comprises a chaos generator.

17. The device of claim 16 wherein said chaos generator implements the following function:

$$f_k(x)=Kx(1-x);$$

where K is a bifurcation parameter of a chaotic system.

18. The device of claim 13, comprising, integrated in one first chip, a logic control unit, a scrambler unit connected to said logic control unit, a chaos generator connected to said logic control unit, a secret storage area storing encryption keys for said scrambler unit and an initial chaotic value for said chaos generator.

19. The device of claim 13, comprising, integrated in a second chip, a logic control unit, an unscrambler unit connected to said logic control unit, a chaos generator connected to said logic control unit, a secret storage area storing encryption keys for said unscrambler unit and an initial chaotic value for said chaos generator.

20. The device of claim 18 wherein said first and said second chips each comprise a coating metal layer covering a respective logic control unit, a respective scrambling/unscrambling unit, a respective chaos generator, and a respective secret storage area.

21. A method to protect the contents of an electronic document, comprising:

acquiring encryption keys and an initial chaotic value;

acquiring input character strings;

generating diffused character strings by calculation using the input character strings, the encryption keys, and previous diffused character strings; and

adding sets of diffused character strings to subsequent chaotic values generated by a chaotic processor to obtain encrypted words.

22. A method to protect the contents of an electronic document, comprising:

acquiring encryption keys and an initial chaotic value;

acquiring input character strings;

calculating diffused character strings using the input character strings, the encryption keys, and previous diffused character strings;

adding sets of diffused character strings to subsequent chaotic values generated by a chaotic processor to obtain encrypted words; and

decrypting the encrypted words by adding the encrypted words to chaotic values identical to the encryption values and subtracted from previously decrypted words using an unscrambler element having a structure similar to that of the scrambler and using identical encryption keys.

23. A method for protecting the contents of an electronic document, comprising:

loading encryption keys into shift registers of an invertible scrambler and an initial chaotic value into a chaotic-value register;

acquiring and input character string;

calculating a diffused character string using the input character string, the encryption keys, and the contents of the shift registers and the following relation:

$$s(t) = IN(t) \oplus \sum_{j=0}^{3} c_j \oplus s(t-j)$$

in which *IN(t)* is said input character string, c_j are said encryption keys, *s(t –j)* are the contents of said shift registers, and *s(t)* is said diffused character string; feeding the diffused character string to the shift registers and issuing a command for a shift operation for the shift registers;

repeating the acquisition of the input character string, calculating the diffused character string, and feeding the diffused character string to the shift registers a predetermined number of times to obtain a plurality of confused character strings;

calculating a subsequent chaotic value using the contents of the chaotic value register; and

adding the plurality of confused character strings to the subsequent chaotic value to obtain an encrypted word.

24. A device for protecting the contents of an electronic document, comprising:

a confusion block for receiving and confusing an electronic input document, the confusion block comprising:

an invertible scrambler that supplies a confused document, the scrambler comprising operators acting within a Galois field, the scrambler comprising an adding element having a first and a second input, the first input receiving a string of characters to be encrypted that belong to the electronic document, a plurality of shift registers cascade-connected to one another and to said adding element, a plurality of multiplier elements, each having an input connected to an output of a shift register and to its own inputs, a plurality of adding nodes cascade-connected, each adding node having an input connected to the output of a respective multiplier element, an adding node arranged upstream and having a second input connected to a second input connected to a last multiplier element of the multiplier elements, and an adding

node arranged downstream and having an output connected to the second input of the adding element; and

a diffusion block cascade-connected to the confusion block, the diffusion block comprising a mixing circuit for mixing the confused document with chaotic characters to supply an encrypted document, the mixing circuit comprising an EXOR logic circuit, and the diffusion block comprising a chaos generator that implements the following function:

$$f_k(x)=Kx(1-x);$$

where K is a bifurcation parameter of a chaotic system.